Introduction to Unification Theory

Solving Systems of Linear Diophantine Equations

Temur Kutsia

RISC, Johannes Kepler University Linz
kutsia@risc.jku.at

ACU-Unification

- We saw an example how to solve ACU-unification problem.
- Reduction to systems of linear Diophantine equations (LDEs) over natural numbers.

Elementary ACU-Unification

- Elementary ACU-unification problem

$$\{f(x, f(x, y)) \doteq^?_{ACU} f(z, f(z, z))\}$$

reduces to homogeneous linear Diophantine equation

$$2x + y = 3z.$$

- Each equation in the unification problem gives rise to one linear Diophantine equation.
- A most general ACU-unifier is obtained by combining all the unifiers corresponding to the minimal solutions of the system of LDEs.

Elementary ACU-Unification

- $\Gamma = \{f(x, f(x, y)) \doteq^?_{ACU} f(z, f(z, z))\}$ and $S = \{2x + y = 3z\}$.
- S has three minimal solutions: $(1, 1, 1), (0, 3, 1), (3, 0, 2)$.
- Three unifiers of Γ:

$$\begin{aligned}\sigma_1 =& \{x \mapsto v_1, y \mapsto v_1, z \mapsto v_1\}\\ \sigma_2 =& \{x \mapsto e, y \mapsto f(v_2, f(v_2, v_2)), z \mapsto v_2\}\\ \sigma_3 =& \{x \mapsto f(v_3, f(v_3, v_3)), y \mapsto e, z \mapsto f(v_3, v_3)\}\end{aligned}$$

- A most general unifier of Γ:

$$\begin{aligned}\sigma = \{&x \mapsto f(v_1, f(v_3, f(v_3, v_3))), y \mapsto f(v_1, f(v_2, f(v_2, v_2))),\\ &z \mapsto f(v_1, f(v_2, f(v_3, v_3)))\}\end{aligned}$$

ACU-Unification with constants

- ACU-unification problem with constants

$$\Gamma = \{f(x, f(x, y)) \doteq^?_{ACU} f(a, f(z, f(z, z)))\}$$

reduces to inhomogeneous linear Diophantine equation

$$S = \{2x + y = 3z + 1\}.$$

- The minimal nontrivial natural solutions of S are $(0, 1, 0)$ and $(2, 0, 1)$.

ACU-Unification with constants

- ACU-unification problem with constants

$$\Gamma = \{f(x, f(x, y)) \doteq^?_{ACU} f(a, f(z, f(z, z)))\}$$

reduces to inhomogeneous linear Diophantine equation

$$S = \{2x + y = 3z + 1\}.$$

- Every natural solution of S is obtained by as the sum of one of the minimal solution and a solution of the corresponding homogeneous LDE $2x + y = 3z$.
- One element of the minimal complete set of unifiers of Γ is obtained from the combination of one minimal solution of S with the set of all minimal solutions of $2x + y = 3z$.

ACU-Unification with constants

- ACU-unification problem with constants

$$\Gamma = \{f(x, f(x, y)) \doteq^?_{ACU} f(a, f(z, f(z, z)))\}$$

reduces to inhomogeneous linear Diophantine equation

$$S = \{2x + y = 3z + 1\}.$$

- The minimal complete set of unifiers of Γ is $\{\sigma_1, \sigma_2\}$, where

$$\begin{aligned}
\sigma_1 = \{&x \mapsto f(v_1, f(v_3, f(v_3, v_3))), \\
&y \mapsto f(a, f(v_1, f(v_2, f(v_2, v_2)))), \\
&z \mapsto f(v_1, f(v_2, f(v_3, v_3)))\} \\
\sigma_2 = \{&x \mapsto f(a, f(a, f(v_1, f(v_3, f(v_3, v_3))))), \\
&y \mapsto f(v_1, f(v_2, f(v_2, v_2))), \\
&z \mapsto f(a, f(v_1, f(v_2, f(v_3, v_3))))\}
\end{aligned}$$

How to Solve Systems of LDEs over Naturals?

Contejean-Devie Algorithm:

Evelyne Contejean and Hervé Devie.
An Efficient Incremental Algorithm for Solving Systems of Linear Diophantine Equations.
Information and Computation 113(1): 143–172 (1994).

Generalizes Fortenbacher's Algorithm for solving a single equation:

Michael Clausen and Albrecht Fortenbacher.
Efficient Solution of Linear Diophantine Equations.
J. Symbolic Computation 8(1,2): 201–216 (1989).

Homogeneous Case

Homogeneous linear Diophantine system with m equations and n variables:

$$\begin{cases} a_{11}x_1 & + \cdots + & a_{1n}x_n & = & 0 \\ \vdots & & \vdots & & \vdots \\ a_{m1}x_1 & + \cdots + & a_{mn}x_n & = & 0 \end{cases}$$

- a_{ij}'s are integers.
- Looking for nontrivial natural solutions.

Homogeneous Case

Example

$$\begin{cases} - x_1 + x_2 + 2x_3 - 3x_4 = 0 \\ - x_1 + 3x_2 - 2x_3 - x_4 = 0 \end{cases}$$

Nontrivial solutions:

- $s_1 = (0, 1, 1, 1)$
- $s_2 = (4, 2, 1, 0)$
- $s_3 = (0, 2, 2, 2) = 2s_1$
- $s_4 = (8, 4, 2, 0) = 2s_2$
- $s_5 = (4, 3, 2, 1) = s_1 + s_2$
- $s_6 = (8, 5, 3, 1) = s_1 + 2s_2$
- $\ldots$

Homogeneous Case

Homogeneous linear Diophantine system with m equations and n variables:

$$\begin{cases} a_{11}x_1 & + \cdots + & a_{1n}x_n & = & 0 \\ \vdots & & \vdots & & \vdots \\ a_{m1}x_1 & + \cdots + & a_{mn}x_n & = & 0 \end{cases}$$

- a_{ij}'s are integers.
- Looking for a basis in the set of nontrivial natural solutions.
- Does it exist?

Homogeneous Case

The basis in the set S of nontrivial natural solutions of a homogeneous LDS is the set of $\gg$-minimal elements S.

$\gg$ is the ordering on tuples of natural numbers:

$$(x_1, \ldots, x_n) \gg (y_1, \ldots, y_n)$$

if and only if

- $x_i \geq y_i$ for all $1 \leq i \leq n$ and
- $x_i > y_i$ for some $1 \leq i \leq n$.

Matrix Form

Homogeneous linear Diophantine system with m equations and n variables:

$$Ax_\downarrow = 0_\downarrow,$$

where

$$A := \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \quad x_\downarrow := \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \quad 0_\downarrow := \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

Matrix Form

- Canonical basis in $\mathbb{N}^n$: $(e_{1\downarrow}, \ldots, e_{n\downarrow})$.
- $e_{j\downarrow} = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}$, with 1 in j's row.
- Then $Ax_\downarrow = x_1 Ae_{1\downarrow} + \cdots + x_n Ae_{n\downarrow}$.

Matrix Form

- a: The linear mapping associated to A.

$$a(x_\downarrow) = \begin{pmatrix} a_{11}x_1 & + \cdots + & a_{1n}x_n \\ \vdots & & \vdots \\ a_{m1}x_1 & + \cdots + & a_{mn}x_n \end{pmatrix} = x_1 a(e_{1\downarrow}) + \cdots + x_n a(e_{n\downarrow}).$$

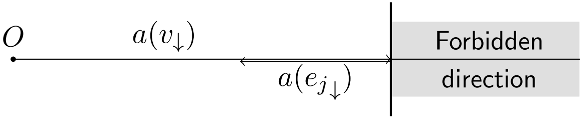
Single Equation: Idea

Case $m = 1$: Single homogeneous LDE $a_1 x_1 + \cdots + a_n x_n = 0$.
Fortenbacher's idea:

- Search minimal solutions starting from the elements in the canonical basis of $\mathbb{N}^n$.
- Suppose the current vector $v_\downarrow$ is not a solution.
- It can be nondeterministically increased, component by component, until it becomes a solution or greater than a solution.
- To decrease the search space, the following restrictions can be imposed:
  - If $a(v_\downarrow) > 0$, then increase by one some v_j with $a_j < 0$.
  - If $a(v_\downarrow) < 0$, then increase by one some v_j with $a_j > 0$.
  - (If $a(v_\downarrow) a(e_{j\downarrow}) < 0$ for some j, increase v_j by one.)

Single Equation: Geometric Interpretation of the Idea

- Fortenbacher's condition
  If $a(v_\downarrow)a(e_{j_\downarrow}) < 0$ for some j, increase v_j by one.
- Increasing v_j by one: $a(v_\downarrow + e_{j_\downarrow}) = a(v_\downarrow) + a(e_{j_\downarrow})$.
- Going to the "right direction", towards the origin.



Single Equation: Algorithm

Case $m = 1$: Single homogeneous LDE $a_1 x_1 + \cdots + a_n x_n = 0$.
Fortenbacher's algorithm:

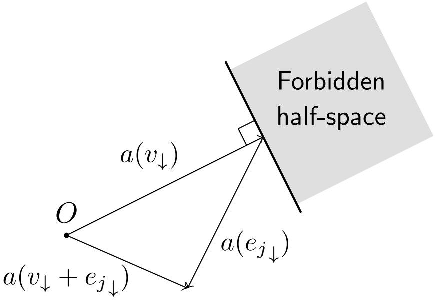
- Start with the pair P, M of the set of potential solutions $P = \{e_{1\downarrow}, \ldots, e_{n\downarrow}\}$ and the set of minimal nontrivial solutions $M = \emptyset$.
- Apply repeatedly the rules:
  1. $\{v_\downarrow\} \cup P', M \Longrightarrow P', M$,
     if $v_\downarrow \gg u_\downarrow$ for some $u_\downarrow \in M$.
  2. $\{v_\downarrow\} \cup P', M \Longrightarrow P', \{v_\downarrow\} \cup M$,
     if $a(v_\downarrow) = 0$ and rule 1 is not applicable.
  3. $P, M \Longrightarrow \{v_\downarrow + e_{j\downarrow} \mid v_\downarrow \in P,\ a(v_\downarrow)a(e_{j\downarrow}) < 0,\ j \in 1..n\}, M$,
     if rules 1 and 2 are not applicable.
- If $\emptyset, M$ is reached, return M.

System of Equations: Idea

- General case: System of homogeneous LDEs.
- $a(x_\downarrow) = 0_\downarrow$.
- Generalizing Fortenbacher's idea:
  - Search minimal solutions starting from the elements in the canonical basis of $\mathbb{N}^n$.
  - Suppose the current vector $v_\downarrow$ is not a solution.
  - It can be nondeterministically increased, component by component, until it becomes a solution or greater than a solution.
  - To decrease the search space, increase only those components that lead to the "right direction".

System of Equations: How to Restrict

- "Right direction": Towards the origin.
- If $a(v_\downarrow) \neq 0_\downarrow$, then do $a(v_\downarrow + e_{j\downarrow}) = a(v_\downarrow) + a(e_{j\downarrow})$.
- $a(v_\downarrow) + a(e_{j\downarrow})$ should lie in the half-space containing O.
- Contejean-Devie condition: If $a(v_\downarrow) \cdot a(e_{j\downarrow}) < 0$ for some j, increase v_j by one. ($\cdot$ is the scalar product.)

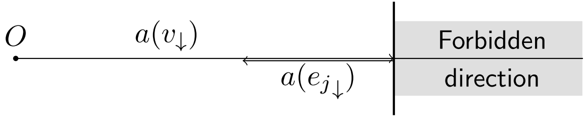


How to Restrict: Comparison

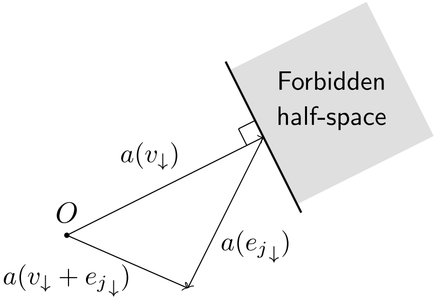
- Fortenbacher's condition
  If $a(v_{\downarrow})a(e_{j_{\downarrow}}) < 0$ for some j, increase v_j by one.
- Contejean-Devie condition
  If $a(v_{\downarrow}) \cdot a(e_{j_{\downarrow}}) < 0$ for some j, increase v_j by one.

How to Restrict: Comparison

Fortenbacher's condition



Contejean-Devie condition



System of Equations: Algorithm

System of homogeneous LDEs: $a(x_{\downarrow}) = 0_{\downarrow}$.

Contejean-Devie algorithm:

- Start with the pair P, M where
  - $P = \{e_{1\downarrow}, \ldots, e_{n\downarrow}\}$ is the set of potential solutions,
  - $M = \emptyset$ is the set of minimal nontrivial solutions.
- Apply repeatedly the rules:

  1. $\{v_{\downarrow}\} \cup P', M \Longrightarrow P', M$,
     if $v_{\downarrow} \gg u_{\downarrow}$ for some $u_{\downarrow} \in M$.
  2. $\{v_{\downarrow}\} \cup P', M \Longrightarrow P', \{v_{\downarrow}\} \cup M$,
     if $a(v_{\downarrow}) = 0_{\downarrow}$ and rule 1 is not applicable.
  3. $P, M \Longrightarrow \{v_{\downarrow} + e_{j_{\downarrow}} \mid v_{\downarrow} \in P,\, a(v_{\downarrow}) \cdot a(e_{j_{\downarrow}}) < 0,\, j \in 1..n\}, M$,
     if rules 1 and 2 are not applicable.

- If $\emptyset, M$ is reached, return M.

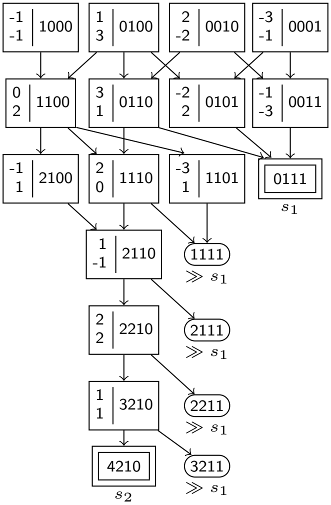
Contejean-Devie Algorithm on an Example

$$\begin{cases} -x_1 + x_2 + 2x_3 - 3x_4 = 0 \\ -x_1 + 3x_2 - 2x_3 - x_4 = 0 \end{cases}$$

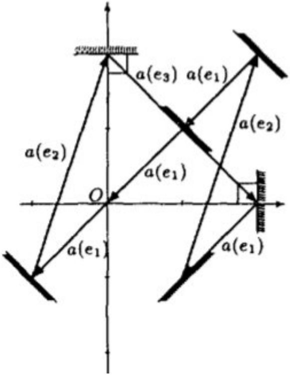
$$e_{1\downarrow} = (1,0,0,0)^T \quad e_{2\downarrow} = (0,1,0,0)^T$$
$$e_{3\downarrow} = (0,0,1,0)^T \quad e_{4\downarrow} = (0,0,0,1)^T$$

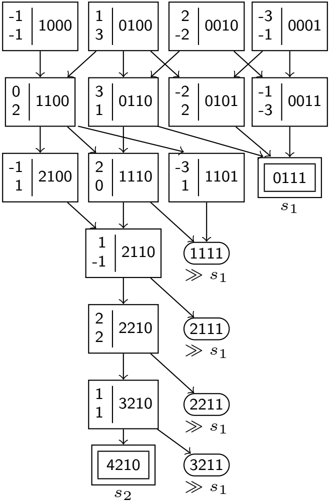
Start: $\{e_{1\downarrow}, \ldots, e_{4\downarrow}\}, \emptyset$.

1. $\{v_\downarrow\} \cup P', M \Longrightarrow P', M$,
   if $v_\downarrow \gg u_\downarrow$ for some $u_\downarrow \in M$.
2. $\{v_\downarrow\} \cup P', M \Longrightarrow P', \{v_\downarrow\} \cup M$,
   if $a(v_\downarrow) = 0_\downarrow$ and rule 1 is not applicable.
3. $P, M \Longrightarrow \{v_\downarrow + e_{j\downarrow} \mid v_\downarrow \in P,$
   $a(v_\downarrow) \cdot a(e_{j\downarrow}) < 0,\ j \in 1..n\}, M$,
   if rules 1 and 2 are not applicable.



Contejean-Devie Algorithm on an Example





Properties of the Algorithm

$a(x_\downarrow) = 0_\downarrow$: An n-variate system of homogeneous LDEs.

$(e_{1\downarrow}, \ldots, e_{n\downarrow})$: The canonical basis of $\mathbb{N}^n$.

$\mathcal{B}(a(x_\downarrow) = 0_\downarrow)$: Basis in the set of nontrivial natural solutions of $a(x_\downarrow) = 0_\downarrow$.

Theorem

- *The Contejean-Devie algorithm terminates on any input.*
- *Let* $(e_{1\downarrow}, \ldots, e_{n\downarrow}), \emptyset \Longrightarrow^* \emptyset, M$ *be the sequence of transformations performed by the Contejean-Devie algorithm for* $a(x_\downarrow) = 0_\downarrow$. *Then*

$$\mathcal{B}(a(x_\downarrow) = 0_\downarrow) = M.$$

Notation

- $\|x_\downarrow\| = \sqrt{x_1^2 + \cdots + x_n^2}$.
- $|(s_1, \ldots, s_n)| = s_1 + \cdots + s_n$.

Completeness

Theorem

Let $P_0, M_0 \Longrightarrow^* \emptyset, M$ *be the sequence of transformations performed by the Contejean-Devie algorithm for* $a(x_{\downarrow}) = 0_{\downarrow}$ *with* $P_0 = (e_{1\downarrow}, \ldots, e_{n\downarrow})$ *and* $M_0 = \emptyset$*. Then* $\mathcal{B}(a(x_{\downarrow}) = 0_{\downarrow}) \subseteq M$*.*

Proof.

Assume $s_{\downarrow} \in \mathcal{B}(a(x_{\downarrow}) = 0_{\downarrow})$ and show that there exists a sequence of vectors

$$v_{1\downarrow} = e_{{j_0}_{\downarrow}} \ll \cdots \ll v_{k\downarrow} \ll v_{k+1\downarrow} = v_{k\downarrow} + e_{{j_k}_{\downarrow}} \ll \cdots \ll v_{|s_{\downarrow}|_{\downarrow}} = s_{\downarrow}$$

such that $v_{i\downarrow} \in P_{l_i}$, where P_{l_i} is from the given sequence of transformations and $l_i < l_j$ for $i < j$.

Completeness

Theorem

Let $P_0, M_0 \Longrightarrow^* \emptyset, M$ *be the sequence of transformations performed by the Contejean-Devie algorithm for* $a(x_\downarrow) = 0_\downarrow$ *with* $P_0 = (e_{1\downarrow}, \ldots, e_{n\downarrow})$ *and* $M_0 = \emptyset$*. Then* $\mathcal{B}(a(x_\downarrow) = 0_\downarrow) \subseteq M$*.*

Proof (cont.)

For $e_{j0_\downarrow}$, any basic vector $\ll s_\downarrow$ can be chosen. Such basic vectors do exist (since $s_\downarrow \neq 0_\downarrow$) and are in P_0. Assume now we have $v_{1\downarrow} \ll \cdots \ll v_{k\downarrow} \ll s_\downarrow$ with $v_{k\downarrow} \in P_{l_k}$. Then there exists $s_{k\downarrow}$ with $s_\downarrow = v_{k\downarrow} + s_{k\downarrow}$ and
$0 = \|a(s_\downarrow)\|^2 = \|a(v_{k\downarrow})\|^2 + \|a(s_{k\downarrow})\|^2 + 2a(v_{k\downarrow}) \cdot a(s_{k\downarrow})$, which implies $a(v_{k\downarrow}) \cdot a(s_{k\downarrow}) < 0$.

Completeness

Theorem

Let $P_0, M_0 \Longrightarrow^* \emptyset, M$ *be the sequence of transformations performed by the Contejean-Devie algorithm for* $a(x_\downarrow) = 0_\downarrow$ *with* $P_0 = (e_{1\downarrow}, \ldots, e_{n\downarrow})$ *and* $M_0 = \emptyset$*. Then* $\mathcal{B}(a(x_\downarrow) = 0_\downarrow) \subseteq M$*.*

Proof (cont.)

Hence, there exists $e_{j_k\downarrow}$ with $s_{k\downarrow} \gg e_{j_k\downarrow}$ such that $a(v_{k\downarrow}) \cdot a(e_{j_k\downarrow}) < 0$. We take $v_{k+1\downarrow} = v_{k\downarrow} + e_{j_k\downarrow}$. Then $s_\downarrow \gg v_{k+1\downarrow}$ and by rule 3, $v_{k+1\downarrow} \in P_{l_{k+1}}$. After $|s_\downarrow|$ steps, we reach s. Hence, $s_\downarrow \in P_{l_{|s|}}$. Since $a(s_\downarrow) = 0$, application of rule 2 moves $s_\downarrow$ to M. □

Soundness

Theorem

Let $P_0, M_0 \Longrightarrow^* \emptyset, M$ *be the sequence of transformations performed by the Contejean-Devie algorithm for* $a(x_\downarrow) = 0_\downarrow$ *with* $P_0 = (e_{1\downarrow}, \ldots, e_{n\downarrow})$ *and* $M_0 = \emptyset$*. Then* $M \subseteq \mathcal{B}(a(x_\downarrow) = 0_\downarrow)$.

Proof.

Any $s_\downarrow \in M$ is a solution. Show that it is minimal. Assume it is not: $s_\downarrow = s_{1\downarrow} + s_{2\downarrow}$, where $s_{1\downarrow}$ and $s_{2\downarrow}$ are non-null solutions smaller than s. Assume $s_\downarrow$ was obtained during the transformations as $s_\downarrow = v_{i\downarrow} + e_{j_i\downarrow}$, where $v_{i\downarrow} \in P_i$. But then $v_{i\downarrow} \gg s_{1\downarrow}$ or $v_{i\downarrow} = s_{1\downarrow}$ or $v_{i\downarrow} \gg s_{2\downarrow}$ or $v_{i\downarrow} = s_{1\downarrow}$ and $v_{i\downarrow}$ is greater than an already computed minimal solution. Therefore, it should have been removed from P_i. A contradiction. $\square$

Termination

Theorem

Let $v_{1\downarrow}, v_{2\downarrow}, \ldots$ *be an infinite sequence satisfying the Contejean-Devie condition for* $a(x_\downarrow) = 0_\downarrow$*:*

- u_1 *is a basic vector and for each* $i \geq 1$ *there exists* $1 \leq j \leq n$ *such that* $a(v_{i\downarrow}) \cdot a(e_{j\downarrow}) < 0$ *and* $v_{i+1\downarrow} = v_{i\downarrow} + e_{j\downarrow}$*.*

Then there exist $v_\downarrow$ *and* k *such that*

- $v_\downarrow$ *is a solution of* $a(x_\downarrow) = 0_\downarrow$*, and*
- $v_\downarrow \ll v_{k\downarrow}$*.*

Non-Homogeneous Case

Non-homogeneous linear Diophantine system with m equations and n variables:

$$\begin{cases} a_{11}x_1 & + \cdots + & a_{1n}x_n & = & b_1 \\ \vdots & & \vdots & & \vdots \\ a_{m1}x_1 & + \cdots + & a_{mn}x_n & = & b_m \end{cases}$$

- a's and b's are integers.
- Matrix form: $a(x_\downarrow) = b_\downarrow$.

Non-Homogeneous Case. Solving Idea

Turn the system into a homogeneous one, denoted S_0:

$$\left\{\begin{array}{ccccccccc} -b_1x_0 & + & a_{11}x_1 & + & \cdots & + & a_{1n}x_n & = & 0 \\ \vdots & & \vdots & & & & \vdots & & \vdots \\ -b_mx_0 & + & a_{m1}x_1 & + & \cdots & + & a_{mn}x_n & = & 0 \end{array}\right.$$

- Solve S_0 and keep only the solutions with $x_0 \leq 1$.
- $x_0 = 1$: a minimal solution for $a(x_\downarrow) = b_\downarrow$.
- $x_0 = 0$: a minimal solution for $a(x_\downarrow) = 0_\downarrow$.
- Any solution of the non-homogeneous system $a(x_\downarrow) = b_\downarrow$ has the form $x_\downarrow + y_\downarrow$ where:
  - $x_\downarrow$ is a minimal solution of $a(x_\downarrow) = b_\downarrow$.
  - $y_\downarrow$ is a linear combination (with natural coefficients) of minimal solutions of $a(x_\downarrow) = 0_\downarrow$.

Back to ACU-Unification

Theorem

The decision problem for ACU-Matching and ACU-unification is NP-complete.